

BEST AVAILABLE CO.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-200195

(43)Date of publication of application : 31.07.1997

(51)Int.Cl.

H04L 9/18

G09C 1/00

H04L 9/34

(21)Application number : 08-010104

(71)Applicant : BROTHER IND LTD

(22)Date of filing : 24.01.1996

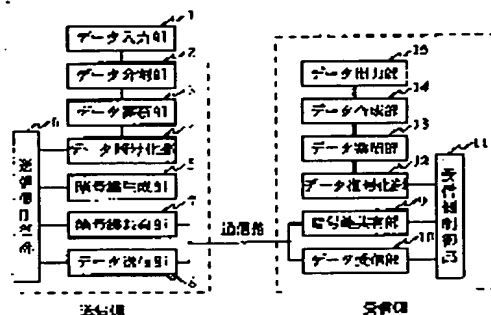
(72)Inventor : NAKAMURA MICHIIRO

(54) CIPHERING COMMUNICATION SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To attain high speed transmission of ciphered data by using a ciphering key so as to apply decode processing to received ciphered data and synthesizing divided data in the order of numbers.

SOLUTION: A transmitter side informs ciphering communication to a receiver side, received transmission data are divided for 512-byte each by a data division section 2 and numbers 1-N are provided to the divided data in the division order and the resulting data are stored in a data storage section 3. The ciphered data are sent from a data transmission section 8 in order. The ciphered data are received by a data reception section 10 and decoded by a decoding section 12 by using a common shared ciphering key and stored in a data storage section 13. The stored data are synthesized in the order of division numbers for each page by a data synthesis section 14. The synthesized data are outputted by a data output section 15 and the entire transmission signal data are outputted finally.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

7

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-200195

(43) 公開日 平成9年(1997)7月31日

| (51) Int.Cl. ⁶ | 識別記号 | 庁内整理番号 | F I | 技術表示箇所 |
|---------------------------|-------|----------|--------------|---------|
| H 0 4 L 9/18 | | | H 0 4 L 9/00 | 6 5 1 |
| G 0 9 C 1/00 | 6 1 0 | 7259-5 J | G 0 9 C 1/00 | 6 1 0 D |
| H 0 4 L 9/34 | | | H 0 4 L 9/00 | 6 8 1 |

審査請求 未請求 請求項の数 3 O L (全 6 頁)

(21) 出願番号 特願平8-10104

(22) 出願日 平成8年(1996)1月24日

(71) 出願人 000005267

ブラザー工業株式会社

愛知県名古屋市瑞穂区苗代町15番1号

(72) 発明者 中村 道弘

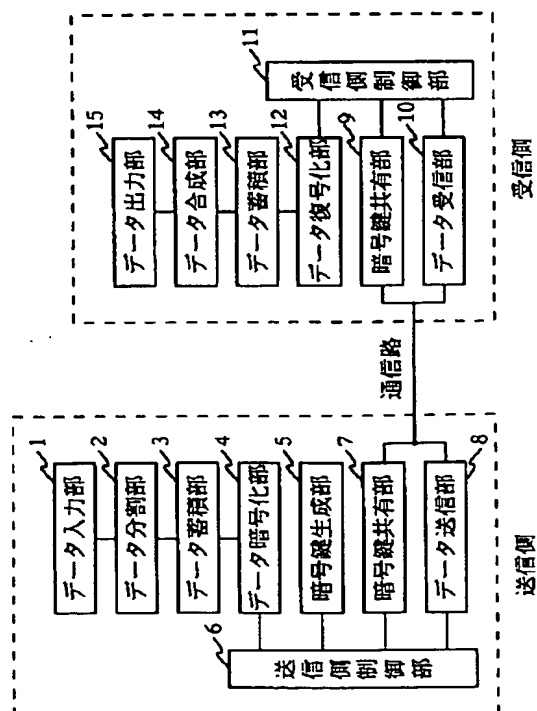
名古屋市瑞穂区苗代町15番1号ブラザー工業株式会社内

(54) 【発明の名称】 暗号通信方式

(57) 【要約】

【課題】 特に大きなデータを暗号化して送信する場合に、送信側と受信側とで高速に暗号化・復号化処理を行うことができ、また、暗号通信の機密性の強度を高めることができる暗号通信方式を提供することである。

【解決手段】 通信時に送信側と受信側とで送信データを暗号化するための暗号鍵を共有し、送信側では、送信データを特定の大きさに分割すると共に、順番に番号を付けて蓄積し、番号が付けられた分割データを暗号鍵を用いて暗号化処理して、受信側にデータの分割数の回数繰り返して送信し、受信側では、受信した暗号化データを暗号鍵を用いて復号処理し、復号された各分割データをデータに付けられた番号順に合成することによって元の送信データに復元する。



【特許請求の範囲】

【請求項1】 データを送信側で暗号化して受信側に送信する暗号通信方式において、

前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記番号が付けられた分割データをそれぞれ暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、

前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成することを特徴とする暗号通信方式。

【請求項2】 データを送信側で暗号化して受信側に送信する暗号通信方式において、

前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記分割数と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを1対1に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、

前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成することを特徴とする暗号通信方式。

【請求項3】 データを送信側で暗号化して受信側に送信する暗号通信方式において、

前記送信側では、送信データを n バイト単位で N 行 \times M 列に分割して、その各列毎に列方向のデータを合成することにより、 $N \times n$ バイトのデータを作成して、各列のデータ毎に i ($1 \leq i \leq M$) の番号を付けて蓄積する一方、その M 列と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを1対1に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記 M 回分繰り返して受信側に送信し、

前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記 N 行 \times M 列に合成することを特徴とする暗号通信方式。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、データを送信側で暗号化して受信側に送信する暗号通信方式に関するものである。

【0002】

【従来の技術】 従来、この種の暗号通信方式においては、データを送信側から受信側に送信する場合、その送信データのデータ全体を送信側で一つの暗号鍵により暗

号化処理した後に受信側に送信されていた。

【0003】

【発明が解決しようとする課題】 しかしながら、従来の暗号通信方式によれば、データ全体を一度に暗号化処理して送信を行うので、特に、容量の大きなデータを送信する場合には、暗号化処理に非常に時間を要し、送信を開始するまでに非常に時間がかかると共に、受信側においても、受信した暗号化データの復号に非常に大きな時間を要する問題点があった。

【0004】 また、データ全体を一つの暗号鍵で暗号化処理を行っていたために、その暗号鍵が知られてしまうと、暗号化データ全体の内容が知られてしまうという問題点があった。

【0005】 本発明は、上述した問題点を解決するためになされたものであり、データを分割した分割データを順次暗号化処理して送信することにより、高速に暗号化データの送信を行うことができる暗号通信方式を提供することである。

【0006】

【課題を解決するための手段】 この目的を達成するために、本発明の請求項1に記載の暗号通信方式は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記番号が付けられた分割データをそれぞれ暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしている。従って、データを分割した分割データを順次暗号化処理して送信することにより、高速に暗号化データの送信を行うことができる。

【0007】 また、請求項2に記載の暗号通信方式は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記分割数と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを1対1に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしている。従って、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性の高い暗号通信を行うことができる。

【0008】 さらに、請求項3に記載の暗号通信方式

は、データを送信側で暗号化して受信側に送信する方式を対象として、特に、前記送信側では、送信データを n バイト単位で N 行 \times M 列に分割して、その各列毎に列方向のデータを合成することにより、 $N \times n$ バイトのデータを作成して、各列のデータ毎に i ($1 \leq i \leq M$)の番号を付けて蓄積する一方、その M 列と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを1対1に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記 M 回分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記 N 行 \times M 列に合成するようにしている。従って、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性の高い暗号通信を行うことができる。

【0009】

【発明の実施の形態】以下に、本発明の暗号通信方式を具体化した実施の形態について図面を参照して説明する。

【0010】図1は本実施の形態における暗号通信方式の構成を示すブロック図である。

【0011】データを送信する送信側は、データ入力部1、データ分割部2、データ蓄積部3、データ暗号化部4、暗号鍵生成部5、送信側制御部6、暗号鍵共有部7、データ送信部8等から構成されている。

【0012】前記データ入力部1は、入力装置（例えば、ファクシミリ装置の読取装置及びコンピュータ等）からのデータを入力するものである。前記データ分割部2は、入力されたデータを512バイト毎のデータに分割するものであり、分割データの最後のものには、ちょうど512バイトになるように付加データとして、アスキーコードの“空白”文字を表わす“0x20”（16進数）を追加して512バイトにする操作をするようにしている。前記データ蓄積部3は、データ分割部2で分割された分割データに分割された順番に分割番号を付けて蓄積するものである。前記データ暗号化部4は、分割番号が付けられた分割データを暗号鍵を用いて暗号化処理するものであり、分割データは分割番号と一緒に暗号化されるものである。前記暗号鍵生成部5は、暗号化処理を行うための暗号鍵を生成するためのものであって、暗号通信を行う度にランダムな暗号鍵を生成するようになっている。

【0013】また、前記送信側制御部6は、送信側の制御処理全体を実行するものであり、データ暗号化処理の制御、暗号鍵生成処理の制御、受信側との暗号鍵共有処理の制御、データ送信処理の制御、通信手順における諸々の制御を実行するものである。前記暗号鍵共有部7は、暗号鍵生成部5で生成された暗号鍵を受信側とで共有するための処理を行うものであり、公開鍵暗号方式を

用いて暗号鍵の共有を行うものである。前記データ送信部8は、データを受信側に送信する処理を行うものである。

【0014】一方、本実施の形態の受信側は、暗号鍵共有部9、データ受信部10、受信側制御部11、データ復号化部12、データ蓄積部13、データ合成部14、データ出力部15等から構成される。

【0015】前記暗号鍵共有部9は、送信側で生成された暗号鍵を通信の際に共有するための処理を行うものである。前記データ受信部10は、送信側から送信されたデータを受信する処理を行うものである。前記受信側制御部11は、受信側の制御処理全体を実行するものであり、送信側との暗号鍵共有処理の制御、データ受信処理の制御、受信データの復号化処理の制御、復号データの合成処理の制御、通信手順における諸々の制御を実行するものである。前記データ復号化部12は、受信データを前記暗号鍵を用いて復号処理するものであり、分割データの個数回復号処理を行うものである。前記データ蓄積部13は、復号処理されたデータを蓄積するためのものである。前記データ合成部14は、復号データを分割番号の順番に合成するためのものである。前記データ出力部15は、前記データ合成部14で合成されたデータを、受信側装置の出力装置に出力するものである。

【0016】図2は本実施の形態における暗号通信方式の送信処理手順を示すフローチャートである。

【0017】先ず、送信側では、コンピュータで作成された送信データがデータ入力部1により入力され（S1、Sはステップを示す。以下同様）、送信者によって暗号通信が選択されれば（S2：Y）、暗号送信手順を行い、暗号通信が選択されなければ（S2：N）、通常の暗号を利用しない通信が行われる。暗号通信の場合には（S2：Y）、受信側との通信接続の際に、暗号通信の通知が受信側に通知される（S3）。入力された送信データは、512バイト毎にデータ分割部2で分割される（S4）。この時、分割されたデータの最後の分割データがちょうど512バイトになるように最終分割データは調節される。ここで、 N 個に分割されたデータは、分割された順番に1～ N の番号が付けられ、図4に示されるようなフォーマットで分割番号が分割データに追加されて、データ蓄積部3に蓄積される（S5）。

【0018】データの暗号化処理に使用される暗号鍵は暗号鍵生成部5で作成され（S6）、暗号鍵共有部7で公開鍵暗号方式を用いて受信側に送信され、受信側と暗号鍵の共有を行う（S7）。この暗号鍵の共有が完了すると、データ暗号化部4において分割番号を含めた分割データを暗号鍵を用いて暗号化処理し（S8）、暗号化された暗号化データを順番にデータ送信部8から送信する（S9）。この時、暗号化処理と暗号化データの送信は同時に動作する処理であり、 n 個目の分割データが暗号化処理されている時には、 $n-1$ 個目の暗号化データ

が送信される。暗号化データの送信が完了すると、終了メッセージを送信して通信を終了する(S10)。

【0019】図3は本実施の形態における暗号通信方式の受信処理手順を示すフローチャートである。

【0020】通信接続の際に暗号通信が通知されると(S21:Y)、受信側の暗号鍵が暗号鍵共有部9で共有され(S22)、暗号化データの受信準備が完了する。

【0021】暗号化データは、データ受信部10によって受信されると共に(S23)、共有された暗号鍵を用いてデータ復号化部12によって復号処理され(S24)、データ蓄積部13に蓄積される。蓄積されたデータは、図4に示すフォーマットであるので、データ合成部14によって分割番号の順番にページ単位毎に合成される(S25)。合成されたデータはデータ出力部15によって出力され(S26)、最終的に送信データ全体を出力することができる。通信終了メッセージを受信すると、通信を終了する(S27)。

【0022】このように、送信データに比べて分割データは小さいので、暗号化処理は短い時間で完了して送信されるので送信開始までの時間を短くすることができ、数ページに亘る文章等の場合には、順次暗号データの復号処理を行うことができ、ページ単位毎に合成を行って出力するので、送信データ全体を一度に暗号化処理するよりも高速に暗号データの送信・出力を行うことができる。

【0023】また、前記実施の形態では、データの分割サイズは512バイトであるが、他の分割サイズでも可能であり、最後の分割データのサイズ調整のためにアスキーコードの“0x20”を使用しているが、“0x00”等の他のコードでも可能である。また、復号データの合成はページ単位で行っているが、復号されたデータを合成せずに順次出力することも可能である。

【0024】また、前記実施の形態では、コンピュータによる暗号通信の場合について述べたが、ファクシミリ通信にこの暗号通信方式を使用することももちろん可能である。

【0025】また、分割データをそれぞれ異なる暗号鍵を用いて暗号化処理を行い、暗号化データとすることも可能である。

【0026】次に、本発明を具体化した他の実施の形態の暗号通信方式について図2及び図3を参照して説明する。

【0027】まず、送信側では、コンピュータで作成された送信データがデータ入力部1により入力され(S1)、送信者によって暗号通信が選択されれば(S2:Y)、暗号送信手順を行い、暗号通信が選択されなければ(S2:N)、通常の暗号を利用しない通信が行われる。暗号通信の場合には(S2:Y)、受信側との通信接続の際に、暗号通信の通知が受信側に通知される(S

3)。入力された送信データを4096バイトと仮定し、行列を1バイト単位として、 $N=64$ 、 $M=64$ とすると、送信データは図5のように示される。この送信データは、データ分割部2において分割処理され(S4)、1列目のデータは、

$D1=M1N1, M1N2, M1N3, \dots, M1N64$

となる。

【0028】以下送信データは、順次64列目のデータまで同様に分割される。

【0029】 $D64=M64N1, M64N2, M64N3, \dots, M64N64$

ここで、これらの64個に分割されたデータは、分割された順番に1~64の分割番号が付けられ、図6のようなフォーマットで分割データに追加されて、データ蓄積部3に蓄積される(S5)。

【0030】データの暗号化処理に使用される暗号鍵は、 $M=64$ 個分だけ暗号鍵生成部5で作成され(S6)、暗号鍵共有部7で公開鍵暗号方式を用いて受信側に送信され、受信側と暗号鍵の共有を行う(S7)。この暗号鍵の共有が完了すると、データ暗号化部4において分割番号を含めた分割データを暗号鍵を用いて暗号化処理し(S8)、暗号化されたデータを順番にデータ送信部8から受信側に送信する(S9)。この時、暗号化処理とデータ送信は同時に動作する処理であり、 n 個目の分割データが暗号化処理されている時には $n-1$ 個目の暗号化データが送信される。暗号データの送信が完了すると終了メッセージを送信して通信を終了する(S10)。

【0031】受信側では、通信接続の際に暗号通信が通知(S21:Y)されると、受信側の暗号鍵が暗号鍵共有部9で共有され(S22)、暗号化データの受信準備が完了する。

【0032】暗号化データはデータ受信部10によって受信され(S23)、送信側と共有された64個の暗号鍵を用いてデータ復号化部12によって復号処理され

(S24)、データ蓄積部13に蓄積される。蓄積されたデータは、列毎のデータ順に並べられているので、データ合成部14では各蓄積データの1バイト目から順番に並び替えることによって全体のデータを合成する(S25)。合成されたデータはデータ出力部15によって出力され(S26)、最終的に送信データ全体を出力することができる。通信終了メッセージを受信すると、通信を終了する(S27)。

【0033】このように、送信データを N 行 \times M 列のデータに分割し、各列毎にデータを合成してひとつの分割データとし、この分割データをそれぞれ異なる暗号鍵を用いて暗号化処理を行うことにより、より暗号強度の高い暗号通信を行うことが可能となる。

【0034】

【発明の効果】以上説明したことから明かなように、本発明の請求項1に記載の暗号通信方式によれば、送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記番号が付けられた分割データをそれぞれ暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしたので、データを分割した分割データを順次暗号化処理して送信することにより、高速に暗号化データの送信を行うことができる。

【0035】また、請求項2に記載の暗号通信方式によれば、送信側では、送信データを特定の大きさに分割して、その分割されたデータに順番に番号を付けて蓄積する一方、前記分割数と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを1対1に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記分割回数分繰り返して受信側に送信し、前記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記番号の順番に従って合成するようにしたので、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性の高い暗号通信を行うことができる。

【0036】さらに、請求項3に記載の暗号通信方式によれば、送信側では、送信データをnバイト単位でN行×M列に分割して、その各列毎にの列方向のデータを合成することにより、N×nバイトのデータを作成して、各列のデータ毎にi (1 ≤ i ≤ M) の番号を付けて蓄積する一方、そのM列と同数の互いに異なる暗号鍵を生成して、それ等の暗号鍵と前記各分割データの番号とを1対1に対応させると共に、前記各分割データをそれぞれ対応する前記暗号鍵を用いて暗号化処理した後、その各暗号化データを前記M回分繰り返して受信側に送信し、前

記受信側では、受信した前記各暗号化データを前記受信側と共有する前記各暗号鍵を用いて復号処理し、その復号された各分割データを前記N行×M列に合成するようにしたので、分割した分割データをそれぞれ異なる暗号鍵で暗号化することにより、データの機密性が一層高い暗号通信を行うことができる。

【図面の簡単な説明】

【図1】本発明の実施の形態における暗号通信方式の構成を示すブロック図である。

10 【図2】暗号通信方式の送信手順を示すフローチャートである。

【図3】暗号通信方式の受信手順を示すフローチャートである。

【図4】暗号通信方式の分割データのフォーマットを示す図である。

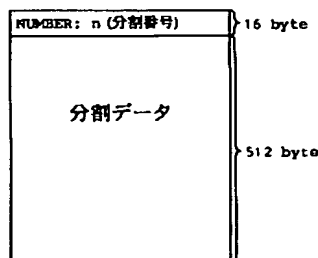
【図5】本発明の他の実施の形態における暗号通信方式のN行×M列の分解データのフォーマットを示す図である。

20 【図6】他の実施の形態における暗号通信方式の分割データのフォーマットを示す図である。

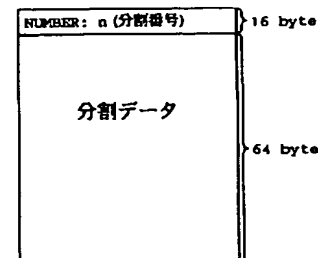
【符号の説明】

- 1 データ入力部
- 2 データ分割部
- 3 データ蓄積部
- 4 データ暗号化部
- 5 暗号鍵生成部
- 6 送信側制御部
- 7 暗号鍵共有部
- 8 データ送信部
- 30 9 暗号鍵共有部
- 10 データ受信部
- 11 受信側制御部
- 12 データ復号化部
- 13 データ蓄積部
- 14 データ合成部
- 15 データ出力部

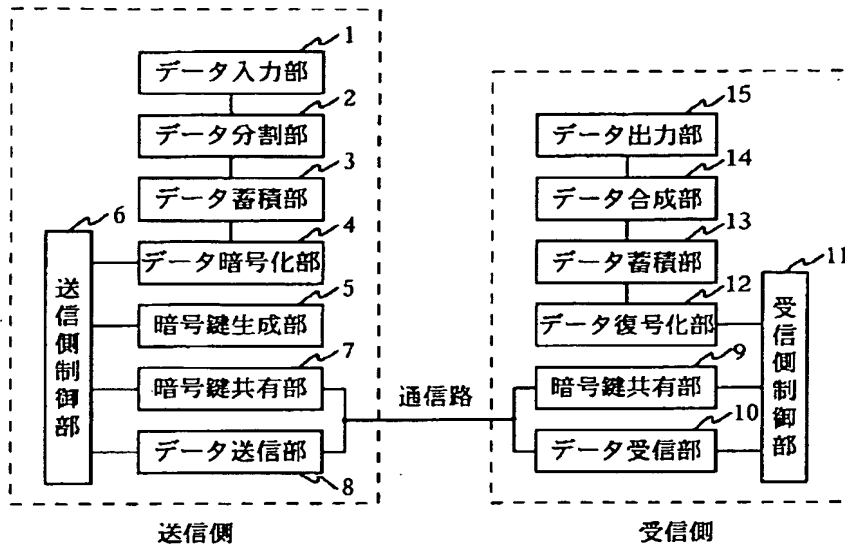
【図4】



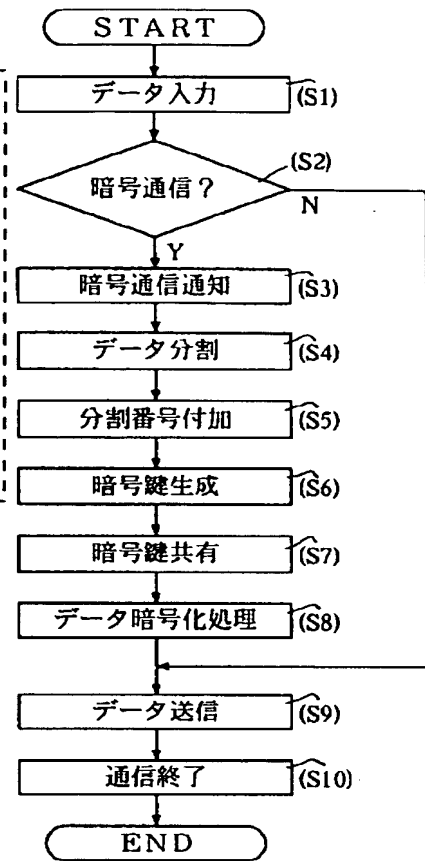
【図6】



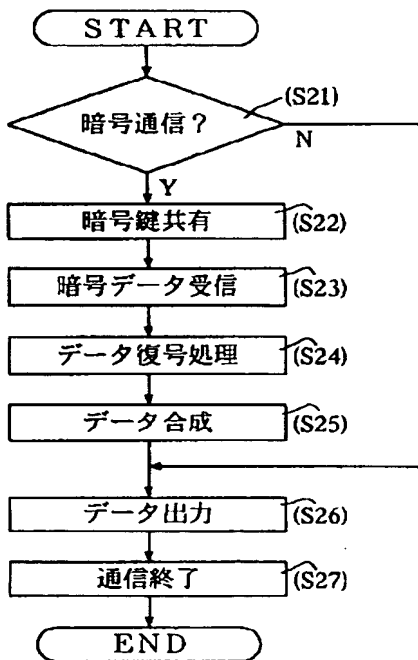
【図 1】



【図 2】



【図 3】



【図 5】

